Faculté des Sciences de Limoges 2002–2003
DESS Sécurité de l'Information
Cryptographie

IP-SEC avec FreeSwan 1

1. Installation

Méthode manuelle

Préparer les sources du noyau et le fichier `.config` adéquat, sans FreeSwan dans un premier temps :

```
# cd /usr/local       % par exemple
# tar -xjf linux-2.x.y.tar.bz2
# cd linux-2.x.y
# make menuconfig     % même si on ne veut pas changer les options
```

Adapter les options présentées par menuconfig (éventuellement). Sortir de menuconfig en **sauvegardant** la configuration, même si elle n'a pas changé, pour qu'un fichier `.config` soit créé. Par prudence : compiler et tester le noyau.

Ajouter FreeSwan :

```
# cd /usr/local   % par exemple
# tar -xzf freeswan-1.x.tar.gz    % trouvé sur www.freeswan.org
# ln -s /usr/local/linux-2.x.y /usr/src/linux
    % ou bien éditer la variable KERNELSRC dans Makefile.inc
# cd freeswan-1.x
# make insert     % pour patcher les sources du noyau
# make programs   % pour compiler les commandes ipsec
# make install    % pour installer les commandes ipsec
```

L'exécutable principal est installé sous le nom `/usr/local/sbin/ipsec` et les sous-commandes dans le répertoire `/usr/local/lib/ipsec/`. Le fichier de configuration et une clé privée RSA sont installés dans `/etc/ipsec.conf` et `/etc/ipsec.secrets`. Si on ne veut pas qu'IP-SEC démarre tout seul, enlever le fichier `/etc/rc.d/ipsec` et le mettre à la place de son lien symbolique `/usr/local/lib/ipsec/setup`.

(Re)ompiler le noyau patché et ses modules. Par défaut, les fonctionnalités IP-SEC sont incluses dans un noyau `ipsec.o` :

```
# cd /usr/local/linux-2.x.y
# make menuconfig   % voir les options FreeSwan dans le menu Networking
# make clean        % ne pas oublier
# make dep
# make bzImage
# make modules
# cp arch/i386/boot/bzImage /<là où on met ses noyaux>/<mon noyau>
# lilo              % avec config adéquate
# rm -Rf /lib/modules/2.x.y
# make modules_install
# shutdown -r now   % voilà, c'est installé
```

Mandrake

C'est peut-être déjà installé. Faire une recherche complète avec le gestionnaire de programmes sur les mots clés *ipsec* et *freeswan* pour installer ce qui manque (deux RPMs : freeswan et kernel-secure). Vous vous retrouverez avec de nouvelles entrées dans le chargeur de boot.

Mais pour que IP-SEC fonctionne sur Mandrake, il faut désactiver la protection anti-spoofing avec quelque chose du genre :

```
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/ipsec0/rp_filter
```

Franchement, je préfère avoir à patcher et recompiler un noyau plutôt que passer des heures à chercher ce genre de détail qui plante tout…

2. Configuration

Les clés

Si vous comptez utiliser des clés symétriques partagées (PSK), inclure une ligne du genre

```
164.81.50.157 164.81.50.48 : PSK "n'importe quoi d'entropie suffisante"
```

et identique sur les deux postes, dans le fichier `ipsec.secrets`.

Echanger les clés publiques RSA des machines concernées (elles ont été générées lors de l'installation). Vous les trouverez à la suite de `#pubkey=` dans les fichiers `/etc/ipsec.secrets`. On peut aussi les obtenir par la commande `ipsec showhostkey`. Recopiez-les dans les fichiers `/etc/ipsec.conf`, aux rubriques `leftrsasigkey=` et `rightrsasigkey=`.

Les options de configuration

Voici un exemple de `ipsec.conf`, définissant un tunnel entre deux postes. Les lignes indentées sont sémantiquement rattachées aux précédentes.

```
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        interfaces=%defaultroute
        klipsdebug=none
        plutodebug=none
        # Use auto= parameters in conn descriptions to control startup actions.
        plutoload=%search
        plutostart=%search
        uniqueids=yes

# defaults for subsequent connection descriptions
conn %default
        keyingtries=0
        authby=rsasig
        auto=add

conn ma-connexion
        left=164.81.50.157
        #leftid=@arnault.unilim.fr
        leftrsasigkey=0s...   (mettre une clé publique)
        right=164.81.50.48
```

```
    #rightid=@truffe18.unilim.fr
    rightrsasigkey=0s...  (mettre une clé publique)
```

Ce fichier est à préparer sur les deux postes et il peut être absolument identique sur ces deux postes. Pour qu'une route IP-SEC soit activée au démarrage du service IP-SEC d'un des postes, on peut remplacer `auto=add` par `auto=start` dans la configuration de ce poste (voire des deux).

Il faut démarrer IP-SEC sur la machine passive (celle avec `auto=add`) par `/usr/local/sbin/ipsec setup --start`, puis démarrer IP-SEC sur la machine active (celle qui va initier la connection, où on a définit `auto=start`). Les deux extrémitées du tunnel sont authentifiées, le tunnel est créé (voir `ifconfig` et `route`) et toute communication est chiffrée.

3. Commandes

Commandes utiles en vrac :

```
ipsec setup [--start | --stop | --restart]    % sans commentaire
ipsec auto --add                              % met en écoute passive
ipsec auto --up                               % active le tunnel déjà chargé
ipsec auto --start                            % charge et active
ipsec auto [--down | --delete | --status]
ipsec eroute                                  % montre les routes chiffrées
ipsec look                                    % infos succintes
ipsec whack --status  % autres info, sur le gestionnaire de clés Pluto
```

4. Ce qu'on peut faire en TP

1. — Installez FreeSwan sur votre distribution (comme indiqué plus haut).

2. — Mettez vous en binôme. Définissez un fichier `ipsec.conf` ressemblant à l'exemple ci-dessus mais en utilisant **vos** adresses IP : `164.81.50.41` à `164.81.50.50` pour `truffe1` à `truffe20` et installez le sur les deux postes (dans `/etc/freeswan/`).

3. — Lancez IP-SEC sur chacun des postes.

```
# ipsec setup --start
```

4. — Ouvrir le tunnel entre les deux postes

```
# ipsec add --up ma-connexion
```

et espérer que le message `IPsec SA established` s'affiche…

5. — Utilisez la connexion et essayez de sniffer avec `ethereal`.

6. — Après, on improvise.